可审核的 CLI 更改事件

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/nas-audit/cli-change-events-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

目录

可审核的 CLI 更改事件 1
可审核的 CLI 更改事件概述 1
管理文件共享事件 2
管理审核策略更改事件 3
管理用户帐户事件 4
管理安全组事件 5
管理 authorization-policy-change 事件 6

可审核的 CLI 更改事件

可审核的 CLI 更改事件概述

ONTAP 可以审核某些命令行界面更改事件，包括某些 SMB 共享事件，某些审核策略事件，某些本地安全组事件，本地用户组事件和授权策略事件。了解可以审核哪些变更事件有助于解释事件日志中的结果。

您可以通过手动轮换审核日志，启用或禁用审核，显示有关审核更改事件的信息，修改审核更改事件以及删除审核更改事件来管理 Storage Virtual Machine （ SVM ）审核 CLI 更改事件。

作为管理员，如果您执行任何命令来更改与 SMB 共享，本地用户组，本地安全组，授权策略和审核策略事件相关的配置， 生成记录并审核相应的事件：

审核类别	事件	事件 IDs	运行此命令 …
Mhost 审核	策略更改	[4719] Audit configuration changed	`vserver audit disable
enable	modify`	文件共享	[5142] Network share was add得
`vserver cifs share create`	[5143] Network share was modified	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] Network share deleted	`vserver cifs share delete`
审核	用户帐户	[4720] 已创建本地用户	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] 已启用本地用户	`vserver cifs users-and-groups local-user create	modify`	[4724] 本地用户密码重置
`vserver cifs users-and-groups local-user set-password`	[4725] 已禁用本地用户	`vserver cifs users-and-groups local-user create	modify`

[4726] 本地用户已删除	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738] Local user Change.	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
【 4781 】本地用户重命名	`vserver cifs users-and-groups local-user rename`	安全组	【 4731 】已创建本地安全组
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734] Local Security Group deleted	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735] Local Security Group Modified
`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] 已将用户添加到本地组	`vserver cifs users-and-groups local-group add-members` `vserver services name-service unix-group adduser`
[4733] 已从本地组中删除此用户	`vserver cifs users-and-groups local-group remove-members` `vserver services name-service unix-group deluser`	authorization-policy-change	【 4704 】已分配用户权限
`vserver cifs users-and-groups privilege add-privilege`	【 4705 】已删除用户权限	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

管理文件共享事件

如果为 Storage Virtual Machine （ SVM ）配置了文件共享事件并启用了审核，则会生成审核事件。使用修改SMB网络共享时会生成文件共享事件 `vserver cifs share` 相关命令。

在为 SVM 添加，修改或删除 SMB 网络共享时，将生成事件 ID 为 5142 ， 5143 和 5144 的文件共享事件。可使用修改SMB网络共享配置 `cifs share access control create|modify|delete` 命令

以下示例显示了在创建名为 "audit_dest" 的共享对象时生成的文件共享事件， ID 为 5143：

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

管理审核策略更改事件

为 Storage Virtual Machine （ SVM ）配置审核策略更改事件并启用审核后，将生成审核事件。使用修改审核策略时会生成audy-policy-change事件 `vserver audit` 相关命令。

无论何时禁用，启用或修改审核策略，都会生成事件 ID 为 4719 的审核策略更改事件，此事件有助于确定用户何时尝试禁用审核以覆盖这些跟踪。默认情况下，它已配置，需要诊断权限才能禁用。

以下示例显示了禁用审核时生成的审核策略更改事件， ID 为 4719：

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

管理用户帐户事件

如果为 Storage Virtual Machine （ SVM ）配置了用户帐户事件并启用了审核，则会生成审核事件。

事件ID为4720、4722、4724、4725、4726的用户帐户事件 在系统中创建或删除本地SMB或NFS用户、启用、禁用或修改本地用户帐户以及重置或更改本地SMB用户密码时、将生成4738和4781。使用修改用户帐户时会生成用户帐户事件 `vserver cifs users-and-groups <local user>` 和 `vserver services name-service <unix user>` 命令

以下示例显示创建本地SMB用户时生成ID为4720的用户帐户事件：

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

以下示例显示了重命名在上述示例中创建的本地SMB用户时生成的ID为4781的用户帐户事件：

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

管理安全组事件

如果为 Storage Virtual Machine （ SVM ）配置了安全组事件并启用了审核，则会生成审核事件。

在系统中创建或删除本地SMB或NFS组时、系统会生成事件ID为4731、4732、4733、4734和4735的安全组事件、并在组中添加或删除本地用户。使用修改用户帐户时会生成secure-group-Events `vserver cifs users-and-groups <local-group>` 和 `vserver services name-service <unix-group>` 命令

以下示例显示了创建本地 UNIX 安全组时生成的 ID 为 4731 的安全组事件：

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

管理 authorization-policy-change 事件

如果为 Storage Virtual Machine （ SVM ）配置了 authorization-policy-change 事件并启用了审核，则会生成审核事件。

每当为 SMB 用户和 SMB 组授予或撤消授权权限时，都会生成事件 ID 为 4704 和 4705 的 authorization-policy-change 事件。使用分配或撤消授权权限时、将生成authorize-policy-change事件 `vserver cifs users-and-groups privilege` 相关命令。

以下示例显示了分配 SMB 用户组授权权限时生成的授权策略事件， ID 为 4704：

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。